Statistiska Centralbyrån

Uppföljning av granskning från 2012

2014-12-16

Building a better working world

Building a better working world

Innehållsförteckning

1. Sammanfattning

Statistiska centralbyråns (SCB) uppgift är att förse regeringen, myndigheter, forskare och kunder inom det privata näringslivet med statistik för beslutsfattande, debatt och allmän information. SCB ansvarar för och framställer officiell statistik inom de ämnesområden som regeringen har beslutat.

Den interna kontrollen över IT-miljön på SCB var föremål för Riksrevisionens granskning redan 2009 vilket föranledde ytterligare granskningar från andra myndigheter och även diskussioner på ministernivå. Detta fick till följd att SCB mottog krav från regeringen att förbättra sitt kvalitetsarbete och införa förordningen (2007:603) om intern styrning och kontroll i verksamheten, något som beslutats om tidigare men inte införts då SCB fått dispens under 2009.

EY genomförde en granskning på uppdrag av Riksrevisionen 2012 med fokus den interna kontrollen för statistikprodukterna Nationalräkenskaperna (NR), Arbetskraftsundersökningarna (AKU), Konsumentprisindex (KPI) samt Betalningsbalansen (BoP). Resultatet av granskningen var ett antal rekommendationer för att stärka den interna kontrollen.

Årets granskning har innefattat en uppföljning av 2012 års rekommendationer. SCB har sedan 2012 vidtagit vissa åtgärder, både på central nivå och på lokal nivå inom respektive enhet, med anledning av de iakttagelser som noterades vid granskningen. Granskningen har visat att SCB vidtagit åtgärder för att möta våra iakttagelser och rekommendationer från 2012. Trots detta kvarstår ett flertal iakttagelser från 2012 helt eller delvis. Vår uppföljande granskning har genomförts under perioden oktober till december 2014.

På en övergripande nivå bedömer vi, liksom vid granskningen 2012, att myndighetens interna kontroll kring förvaltningen av de IT-system som stödjer statistikproduktionen i flera avseenden har väl utformade och definierade kontroller som, om de utförs som beskrivet, bidrar till en god kontrollmiljö. Sedan granskningen 2012 har vi har sett förbättringar i SCB:s interna kontroll framförallt kring dokumentation och spårbarhet i utförandet av kontroller. Det finns dock ett fortsatt utrymme för förbättring avseende efterlevnaden av nyligen införda rutiner samt avseende spårbarheten i kontrollutförandet inom vissa områden.

Våra huvudsakliga sammanfattade iakttagelser beskrivs nedan, de beskrivs vidare i Avsnitt 4:

- Statistikproduktionen innehåller manuella överföringar av information mellan olika filer
- Tvingande ansvarsfördelning vid produktionssättning av programförändringar saknas på grund av avsaknad av enhetliga testmiljöer
- Spårbarheten vid programförändringar med avseende på Excel-filer och SAS-script är i flera avseenden otillräcklig vilket innebär att det inte går att i efterhand granska att genomförda förändringar testats och godkänts innan de tagits i bruk.

2. Inledning

2.1 Uppdrag

Riksrevisionen har som en del av den årliga revisionen av SCB uppdragit åt EY att göra en uppföljning av 2012 års granskning gällande SCB:s interna kontroll i de IT-processer som stödjer statistikproduktionen för produkterna Arbetskraftsundersökningen (AKU), Betalningsbalansen (BoP), Nationalräkenskaperna (NR) samt Konsumentprisindex (KPI). Granskningen har innefattat en uppföljning av rekommendationerna från granskningen 2012. Uppdraget utförs som avrop på "Avtal avseende Revisionstjänster årlig revision mellan Riksrevisionen och Ernst & Young AB " dnr 38-2011-1507

2.2 Genomförande

Granskningen har genomförts med utgångspunkt i våra rekommendationer från 2012 års granskning, se bilaga 1 till Riksrevisonens rapport: *Granskning av den interna kontrollen i bearbetningsprocessen för framtagandet av väsentliga produkter hos Statistiska centralbyrån*, dnr: 32-2012-0562. Granskningen inleddes genom en översiktlig kartläggning av de åtgärder som SCB vidtagit sedan 2012. I de fall SCB vidtagit omfattande åtgärder sedan 2012 har en ny kartläggning av processen för statistikproduktion genomförts. Vidare verifierades huruvida de kontroller, för vilka SCB vidtagit åtgärder sedan 2012, fungerar som avsett. Verifiering genomfördes genom att utföra test av ett lämpligt urval av de identifierade kontrollerna.

Arbetet har genomförts genom intervjuer och granskning av tillhandahållen dokumentation. Se bilaga A för en översikt över respondenter och granskade dokument. Uppdragets genomfördes under perioden oktober till december 2014.

2.3 Omfattning

Detta dokument beskriver vår granskning och bedömning av nyckelkontroller som omfattats av rekommendationer i 2012 års granskning. För varje rekommendation har vi beskrivit status vid årets granskning samt vår bedömning huruvida rekommendationen är åtgärdad. Rapporten innehåller även vidare rekommendationer i de fall vi identifierat ytterligare förbättringspotential. Våra iakttagelser med tillhörande riskbeskrivningar och rekommendationer är avsedda att utgöra ett stöd för SCB:s verksamhet.

2.4 Avgränsningar

Vår granskning är avgränsad till de områden som omfattats av 2012 års rekommendationer. Vår granskning har inte haft sådan omfattning eller inriktning att vi haft möjlighet att upptäcka alla brister, oegentligheter eller andra avvikelser som kan förekomma. Kontroller och rutiner kan heller aldrig utgöra ett fullständigt skydd mot försummelser eller mot oegentligheter som utförs av flera personer i samarbete.

3. Granskning av statistikprodukterna

3.1 Nationalräkenskaperna

3.1.1 Processen för statistikproduktion

Processen för statistikproduktionen för Nationalräkenskaperna (NR) är väsentligen oförändrad sedan granskningen som genomfördes 2012. För detaljerad processbeskrivning se bilaga 1 till Riksrevisionens rapport: Granskning av den interna kontrollen i bearbetningsprocessen för framtagandet av väsentliga produkter hos Statistiska centralbyrån, dnr: 32-2012-0562.

3.2 Konsumentprisindex

3.2.1 Processen för statistikproduktion

Processen för statistikproduktionen för Konsumentprisindex (KPI) är väsentligen oförändrad sedan granskningen som genomfördes 2012. För detaljerad processbeskrivning se bilaga 1 till Riksrevisionens rapport: Granskning av den interna kontrollen i bearbetningsprocessen för framtagandet av väsentliga produkter hos Statistiska centralbyrån, dnr: 32-2012-0562.

3.3 Arbetskraftsundersökningarna

3.3.1 Processen för statistikproduktion

Processen för statistikproduktionen för Arbetskraftsundersökningarna (AKU) är väsentligen oförändrad sedan granskningen som genomfördes 2012. För detaljerad processbeskrivning se bilaga 1 till Riksrevisionens rapport: Granskning av den interna kontrollen i bearbetningsprocessen för framtagandet av väsentliga produkter hos Statistiska centralbyrån, dnr: 32-2012-0562.

3.4 Betalningsbalansen

3.4.1 Processen för statistikproduktion

Betalningsbalansen (BoP) är en sammanställning av Sveriges reala och finansiella transaktioner gentemot utlandet. Enheten BFM på SCB producerar betalningsbalansen på uppdrag av Riksbanken.

Det tidigare centrala systemet för sammanställning av beräkningar, Buster, är under avveckling och är i takt med att ersättas av FMBoP. Fler av beräkningsdelarna kommer lyftas in i FMBoP för att minska arbetet i Excel-mallar.

Nedan följer en beskrivning av hur statistiken produceras baserat på vår förståelse av processen under granskningen. I processkartan illustreras de huvudsakliga processtegen samt identifierade nyckelkontroller.

Insamling
Enheten som producerar betalningsbalansen samlar in primärstatistik till den finansiella balansen samt avkastning via ett trettiotal blanketter. Den övervägande delen samlas in månadsvis via Excelblanketter som är tillgängliga för uppgiftslämnare på företag via Internet. Dessa blanketter läses in via automatisk överföring och laddas in via schemalagda jobb i FMBoP, för vissa inlämnade uppgifter används fortfarande Buster som första steg innan inläsning i FMBoP.

Inrapportering för Direktinvesteringsenkäten (DI-enkäten) som är en årlig urvalsundersökning sker genom att webb-blanketter via systemet SIV läses in i systemet DiÅr. Då undersökningen är en urvalsundersökning körs SAS-program som räknar upp resultatet för att gälla hela populationen. Efter att uppgifterna har granskats körs ett skript som tar fram underlag till IT för inläsning av information i Buster.

BFM tar även emot viss data från externa källor utanför SCB. Dessa används som underlag i beräkningsfiler i Excel. Dessa filer tar även input direkt från Buster. Beräknad data blir åter indata till Buster och läses in i systemet automatiskt från en mapp på en filarea.

Beräkning

BFM har ett tjugotal Excel-filer som används för beräkningar av olika poster i betalningsbalansen. I dagsläget används både Buster och FMBoP för beräkning inom BoP. Sedan FMBoP infördes används Buster för att säkerställa att beräkningarna i FMBoP är korrekta. Data som läses in i FMBoP och DiÅr granskas via fördefinierade rapporter från verktyget SAS Webb report studio (WRS). När uppgifter och blanketter är godkända markeras detta i FMBoP och de förs då över till beräkningsdatabasen. Om felaktigheter upptäcks spåras felet tillbaka till uppgiftslämnaren för att korrigeras eller kompletteras.

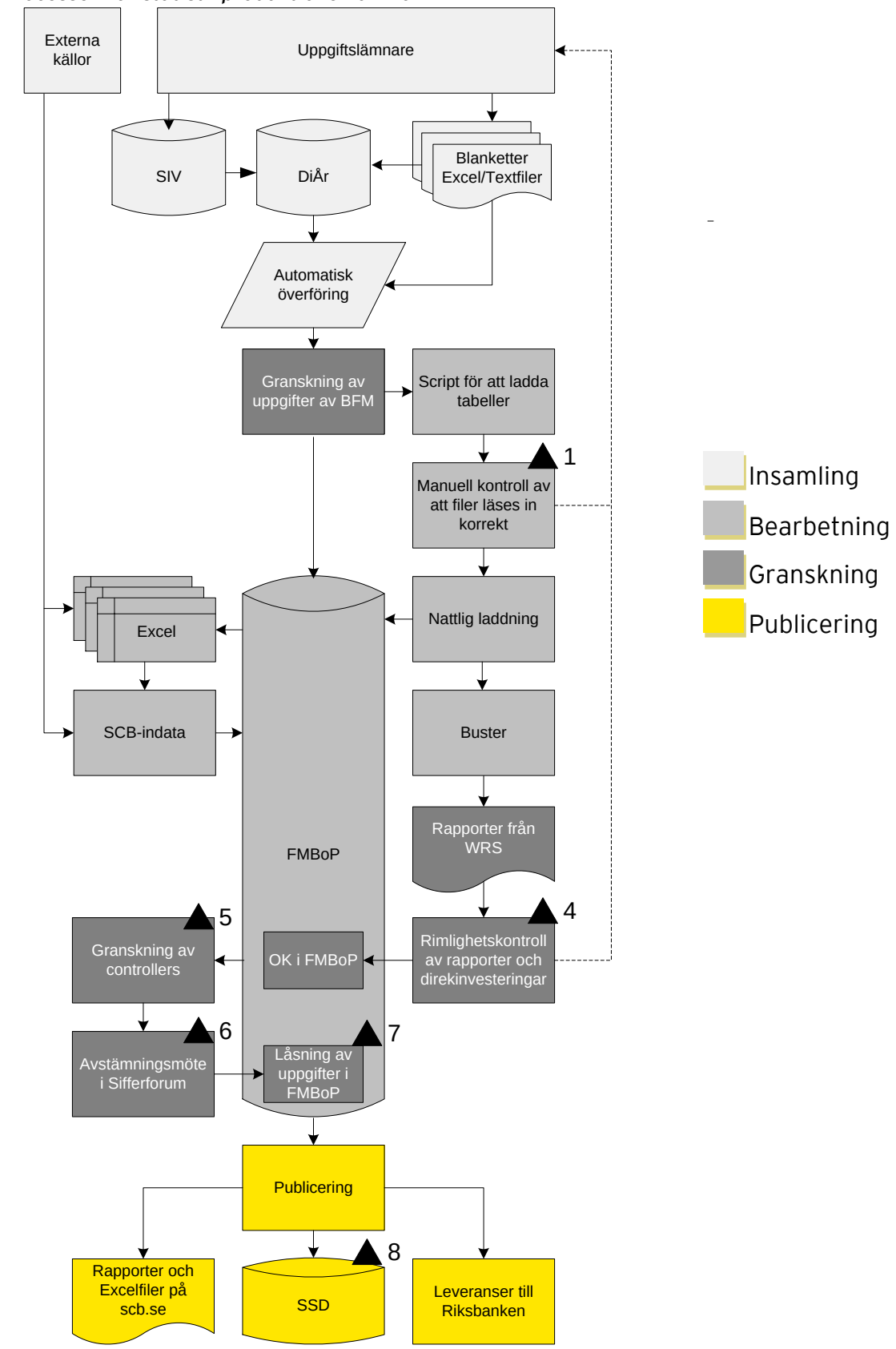
Granskning

Data granskas på mikronivå och två controllers ansvarar sedan för en avstämning på makronivå. I granskningens slutfas diskuteras utfallet på "Sifferforum" och därefter låses siffrorna och får status tillfällig publiceringsstruktur (TPS). Den tillfälliga publiceringsstrukturen markeras i FMBoP. Anteckningar från mötet sparas på en gemensam filyta.

Publicering

Controllers initierar definitivkörningen av den tillfälliga publiceringsstrukturen i Buster. Rapporter beräknas enligt fördefinierade beräkningsmodeller beroende på mottagare och ändamål. Huvuddelen av materialet som publiceras på scb.se är i form av Excel-filer och rapporter. Data till Excelfilerna hämtas via verktyget Excel-nätdata från en central fil som skapas vid varje kvartalsutdrag för att minimera risken för manuella fel. Diagram från Excel-filerna kopieras in i rapporterna.

Processen för statistikproduktionen av BoP



4. Iakttagelser och rekommendationer

EY har identifierat ett antal förbättringsområden i samband granskningen. Samtliga observationer och tillhörande rekommendationer har klassificerats utifrån följande skala:

Prioritet 1 – Risken bör hanteras snarast.

Prioritet 2 – Risken bör hanteras inom en snar framtid.

Prioritet 3 – Förbättringsområde som bör hanteras på sikt.

4.1 Övergripande iakttagelser

4.1.1 Statistikproduktionen innehåller manuella överföringar av information mellan olika filer

Iakttagelse 2012
Inom samtliga granskade statistikprodukter ingår det steg vid statistikproduktion som innebär att siffror manuellt kopieras eller på annat sätt överförs från en fil till en annan. Vi har vid vår granskning sett exempel på när sådana överföringar lett till fel i den publicerade statistiken som upptäckts först i efterhand.

Status 2014
Vid vår uppföljning noterade vi att processerna för statistikproduktion är väsentligen oförändrade vilket innebär att manuella överföringar kvarstår. Inom flera statistikområden finns en ambition att minska de manuella överföringarna och användning av Excel. Än så länge är dock processen präglad av manuella överföringar i vissa delmoment.

Risk 2014 – Prioritet 1
Manuella överföringar av information mellan filer ökar risken för oavsiktliga fel på grund av tillfälliga tekniska brister eller handhavandefel.

Rekommendation 2014
Vi bedömer att iakttagelsen från 2012 kvarstår. Många manuella överföringar kvarstår och vi rekommenderar att SCB ser över sina centrala riktlinjer och krav på statistikproduktionen för att minska användandet av manuella överföringar av information i statistikproduktionsprocesserna.

4.1.2 Den centrala regelbundna granskningen av behörigheter i Active Directory är otillräcklig

Iakttagelse 2012
SCB genomför årligen en centralt koordinerad genomgång av behörigheter i Active Directory. Denna genomgång bygger på en lista som manuellt sammanställs inför varje omgång. Vid vår granskning noterade vi att det saknades vissa behörighetsgrupper i granskningen – vilket inte uppmärksammats vid genomgången. Vi noterade även att listan inte visar vilka användare och grupper som faktiskt har behörighet till respektive avdelnings nätverksmappar. Detta innebär att användare som fått behörighet till en viss mapp eller äldre grupper som inte längre borde vara i bruk fortfarande kan ha åtkomst till filer och mappar utan att det upptäcks vid granskningen. Vidare noterade vi att resultatet av granskningen inte dokumenteras.

Status 2014
Vid vår granskning noterade vi att SCB har infört centrala rutiner för behörighetsgenomgången av Active Directory. En gång per år görs ett utdrag ur Active Directory med användare på hela SCB,

utdraget bygger på grupptillhörighet som granskas och lämnas till säkerhetsorganisationen. Säkerhetsorganisationen ansvarar för att listan ska skickas ut till respektive enhetschef som granskar listan utifrån vilka medarbetare som bör ha behörigheter, därefter markerar enhetschefen sitt godkännande eller lämnar kommentar om korrigerande åtgärd. När behörigheterna har granskats av respektive enhetschef skickas listorna tillbaka till säkerhetsorganisationen som arkiverar informationen och vidtar eventuella korrigerande åtgärder. Vid våra stickprov noterade vi att SCB inte regelmässigt granskar att användares behörighetsnivå är lämplig utifrån användarens yrkesroll. I de flesta fall granskas enbart huruvida användaren arbetar inom avdelningen eller ej.

Rekommendation 2014
Vi bedömer att iakttagelsen från 2012 är åtgärdad. Vi rekommenderar dock vidare att SCB stärker kontrollen genom att även kontrollera att användares behörighetsnivå är lämplig utifrån användarens yrkesroll.

4.1.3 Den centrala regelbundna granskningen av behörigheter i databaser dokumenteras inte

Iakttagelse 2012
Enligt SCB genomförs en regelbunden central genomgång av behörigheter i SCB:s databaser. Vid vår granskning noterade vi att denna genomgång inte är dokumenterad och därför har vi inte kunnat bekräfta att granskningen genomförs.

Status 2014
Vid vår granskning 2014 noterade vi att SCB har infört ägare på samtliga databaser. Vid den årliga behörighetsrevisionen ansvarar ägaren för databasen för att granska behörigheter i respektive databas. Samtliga filer för behörighetsgenomgången ska enligt rutinen sparas på en central plats. Vid vår granskning observerade vi även att SCB genomfört en databasrevision av samtliga databaser, med syfte att rensa bort databaser som inte längre är i bruk.

Rekommendation 2014
Vi bedömer iakttagelsen från 2012 som åtgärdad.

4.1.4 Lösenordet till det inbyggda administratörskontot byts inte regelbundet

Iakttagelse 2012
Vid vår granskning noterade vi att lösenordet till det inbyggda Administratörskontot i Active Directory är skyddat både i kassaskåp och i en krypterad databas. Vi noterade dock att lösenordet inte byts med jämna mellanrum.

Status 2014
Vi noterade att SCB har åtgärdat iakttagelsen i samband med vår granskning 2014. SCB har dokumenterat och infört en rutin daterad 2014-12-03 för att regelbundet byta lösenordet till administratörskontot. Vi har därefter noterat att SCB genomfört rutinen som beskrivet.

Rekommendation 2014
Vi bedömer vår iakttagelse från 2012 som åtgärdad med hänsyn till de åtgärder som genomförts under granskningen.

4.1.5 Användare med domänadministratörsbehörighet har tilldelats i fel grupp

Iakttagelse 2012
SCB tilldelar som regel domänadministratörsbehörigheter till grupper där användare läggs in beroende på sin organisatoriska tillhörighet. Vid vår granskning noterade vi att användare lagts till direkt som domänadministratör istället för att tilldelas behörighet via sin grupp. Vidare noterade vi en användare i en grupp där inaktiva användarprofiler sparas som fortfarande var aktiv.

Status 2014
Vid vår uppföljning noterade vi att SCB har förändrat denna rutin så att behörigheter ska tilldelas efter grupptillhörighet och inte på individnivå. Vid vår granskning noterade vi dock att enstaka användare fortfarande tilldelats behörigheter på individnivå utanför gällande rutin. I detta fall gavs användaren inte vidare behörighet än vad användaren hade rätt till. Individuell tilldelning av behörigheter utanför de avsedda behörighetsgrupperna ökar dock risken och komplexiteten vid framtida förändring av behörighet.

Risk 2014 – Prioritet 2
Genom att användare tilldelats behörigheter på andra sätt än enligt gängse rutiner eller placerats i felaktiga grupper ökar risken för att behörigheten inte upptäcks eller tas bort inom rimlig tid så den inte tilldelats där man förväntat sig eller har tilldelats dubbelt.

Rekommendation 2014
Vi bedömer att vår iakttagelse från 2012 är delvis åtgärdad. Vi rekommenderar att SCB fortsätter införandet av en rutin för att med jämna mellanrum granska systemadministratörsbehörigheter för att säkerställa att ingen tilldelats behörighet på felaktigt sätt.

4.1.6 Ansvarsfördelning vid produktionssättning av programförändringar saknas

Iakttagelse 2012
Vid vår granskning noterade vi att det i samtliga statistikprodukter regelmässigt är de som utvecklat förändringar i system, skript och Excel-filer som också driftsätter förändringarna.

Status 2014
SCB arbetar på en ny rutin samt att bygga en egen utvecklingsmiljö. Vid granskningstillfället hade dock inga åtgärder tillämpats.

Risk 2014 – Prioritet 2
Bristen på ansvarsfördelning vid produktionssättning av programförändringar ökar risken för att processen för programförändringar kringgås och att oönskad funktionalitet eller otillräckligt testade och felaktiga förändringar införs i produktionsmiljön. Detta i sin tur leder till en ökad risk för fel i de statistiska beräkningarna.

Rekommendation 2014
Vår bedömer att vår iakttagelse från 2012 kvarstår, att SCB inför riktlinjer som innebär att utvecklare regelmässigt inte har skrivbehörigheter i produktionsmiljön. I den mån sådana behörigheter behövs för felsökning eller motsvarande rekommenderar vi att en rutin införs för att tillfälligt låsa upp konton med skrivbehörighet för enstaka tillfällen.

4.1.7 Kontroller kring fysisk åtkomst till datahallarna kan förbättras

Iakttagelse 2012
Vid vår granskning noterade vi att behörigheter till datahallen i Örebro i vissa fall inte tagits bort när medarbetare slutat eller bytt roll. Vidare noterade vi att vissa leverantörer använder sig av personliga kort vid tillträde till datahallen. Kortsystemet till datahallen stödjer loggning av vilka kort som använts och när men vi noterade att ingen regelbunden uppföljning av inpasseringar genomförs.

Status 2014
Under vår uppföljning noterade vi att SCB tagit fram ett styrdokument som beskriver rutinen för hantering av fysisk behörighet till datahallarna. Rutinen innebär att en loggbok förs över inpassering i datahallarna. Vidare reglerar styrdokumentet att alla passerkort skall vara personliga samt att en behörighetsgenomgång skall genomföras två gånger per år, i mars och september. Behörighetsgenomgången dokumenteras i loggboken tillsammans med nästa planerade datum för genomförande.

Rekommendation 2014
Vi bedömer iakttagelsen som åtgärdad.

4.1.8 Test av strömförsörjning i datahallarna dokumenteras inte

Iakttagelse 2012
Enligt uppgift från SCB testas regelbundet den utrustning som ska ge reservström till datahallarna vid händelse av strömavbrott. Dessa tester dokumenteras inte vilket försvårar uppföljning av när tester senast utfördes och vad resultatet blev.

Status 2014
Vid vår granskning noterade vi att strömförsörjningstester genomförts och dokumenterats. Det senast genomförda testet påvisade ett antal förbättringspunkter för att säkerställa kontinuitet i driften.

Rekommendation 2014
Vi bedömer att vår iakttagelse från 2012 som åtgärdad. Vi rekommenderar dock att SCB vidtar åtgärder på de anmärkningar som uppkommit vid test av strömförsörjningen.

4.2 Nationalräkenskaperna

4.2.1 Spårbarheten vid programförändringar i NR-Systemet, SAS-skript och Excel-filer är otillräcklig

Iakttagelse 2012
Vid vår granskning noterade vi att det inte var möjligt att få ut en tillförlitlig förteckning över de programförändringar som genomförts i NR-systemet under året. Vidare noterade vi att beställningar, tester och godkännanden av programförändringar inte regelmässigt dokumenteras och sparas. Vi noterade dock att en ny förvaltningsrutin tagits fram som har potential att åtgärda iakttagelsen men att den ännu inte tagits i bruk. I de fall dokumenterade testfall används noterade vi att dokumentationen inte var tillräcklig för att avgöra vad ett genomfört test berör och vilka förändringar som faktiskt genomgått godkänt test. I samband med Excel-projektet genomgick inte alla Excel-filer slutligt acceptanstest.

Status 2014
Vid vår granskning noterade vi att NR infört nya rutiner samt ett nytt ärendehanteringssystem för att hantera och dokumentera programförändringar. Våra stickprov påvisade dock att rutinen inte alltid efterlevs för samtliga programförändringar.

Risk 2014 – Prioritet 2
Bristande efterlevnad av, och spårbarhet i, programförändringsprocessen ökar risken för oönskad funktionalitet eller att otillräckligt testade och felaktiga förändringar utvecklas och införs i produktionsmiljön. Detta i sin tur leder till en ökad risk för fel i de statistiska beräkningarna.

Rekommendation 2014
Vi bedömer att vår iakttagelse från 2012 är delvis åtgärdad. Vi rekommenderar att NR fortsätter arbetet med att införa den nya förvaltningsmodellen och säkerställa att den efterlevs för alla typer av programförändringar.

4.2.2 Behörigheter har tilldelats i Active Directory och i NR-Systemet utan underlag

Iakttagelse 2012
Vid vår granskning noterade vi att behörigheter i Active Directory och NR-Systemet har lagts till under året men att motsvarande beställning saknades eller inte gick att hitta. Vidare noterade vi att den manuella förteckningen över behörigheter som upprättats inte överensstämde med de faktiska behörigheter som var aktiva i systemet. Detta innebär att de genomgångar av behörigheter som genomförts med stöd av den manuella förteckningen inte har haft förutsättningar att identifiera obehöriga användare.

Status 2014
SCB har infört centrala rutiner för behörighetshanteringen till Active Directory. Rutinen innebär att behörigheter till Active Directory beställs genom Beställarportalen, en webbtjänst på SCB:s intranät. Ägaren för respektive grupp skall godkänna beställningar. I de fall gruppägaren är frånvarande och behörigheter måste godkännas omedelbart har Nationalräkenskapssystemets förvaltningsansvarig och kvalitetssystemansvarig rättigheter att hjälpa till med akuta behörighetsärenden. Se även iakttagelse 4.1.2 för den nya centrala rutinen av uppföljning av behörigheter i Active Directory. För nya behörigheter till databaser följs inte beställningsrutinen som för Active Directory, där går beställningen via e-post.

Rekommendation 2014
Vi bedömer vår iakttagelse från 2012 som åtgärdad.

4.2.3 Skyddet som används för Excel-filer hindrar inte oavsiktliga fel

Iakttagelse 2012
NR använder ett så kallat mjukt skydd av de Excel-filer som används vid statistikproduktion för att försvåra oavsiktliga förändringar. Skyddet innebär att filerna öppnas skrivskyddade från början och en användare måste aktivt välja att stänga av skyddet för att kunna ändra i filerna. För att kunna arbeta med statistiken är det nödvändigt att avaktivera skrivskyddet för att föra in statistikuppgifterna i arket – därmed kan oavsiktliga fel uppstå i samband med det löpande arbetet. Vi noterade även att användarna kopierar Excel-fil som användes vid den senaste produktionen när det är dags att uppdatera för den nya månaden.

Status 2014
Vi noterade att i samband med omläggningen till Europeiska Nationalräkenskapssystemet har SCB infört cellskydd i Excel-filerna som används för uträkningarna av BNP per kvartal. Man har dock valt att inte införa detta i andra delar av statistikproduktionen då målet är att lyfta in alla beräkningar i det nya IT-systemet och på längre sikt avveckla arbetet i Excel.

Risk 2014 – Prioritet 2
Genom att skyddet måste avaktiveras för att den ansvarige ska kunna utföra sitt arbete hindrar inte skyddet oavsiktliga fel som uppstår inom ramen för statistikproduktionen, med undantag för det skydd som införts för BNP per kvartal. Att kopiera den senast använda filen innebär också en ökad risk för att oavsiktliga fel som införts består genom flera omgångar då man inte utgår från en kontrollerad och godkänd originalfil.

Rekommendation 2014
Vi bedömer att iakttagelsen från 2012 kvarstår, med undantag för BNP kvartal där vi bedömer iakttagelsen från 2012 som åtgärdad. Vi rekommenderar att NR fortsätter införa skydd på cellnivå i de Excel-filer som innehåller formler eller länkar, så att enbart de celler som är avsedda för inmatning av data kan ändras. Vidare rekommenderar vi att NR upprättar testade och godkända originalfiler som används som underlag vid ny statistikproduktion för att förhindra att oavsiktliga fel kvarstår över tid. Vi rekommenderar även att SCB fortsätter att avveckla arbetet i Excel för att föra över det till det nya IT-systemet.

4.3 Konsumentprisindex

4.3.1 Spårbarheten vid programförändringar i SAS-skript och Excel-filer är otillräcklig

Iakttagelse 2012
Vid vår granskning noterade vi att det inte var möjligt att få ut en tillförlitlig förteckning över de programförändringar som genomförts i SAS-skript och Excel-filer under året. Vidare noterade vi att beställningar, tester och godkännanden av programförändringar inte regelmässigt dokumenteras och sparas.

Status 2014
Vid vår uppföljning noterade vi att SCB har implementerat en generell checklista för programförändringar i Pi09. Checklistan har anpassats för kvalitetssäkringssystemet Tekla. SCB har även ett detaljerat dokument för beställare, ändringsansvarig och testansvarig som är färgkodat för att respektive person enkelt ska kunna se vilka uppgifter som ska fyllas i.

Vi noterade även att Excel-filerna för KPI skrivskyddade, vilket minskar risken för att ändringar sker av misstag. Det finns dock ännu inte tillräcklig spårbarhet för förändringar som genomförs i Excelberäkningsfiler och SAS-script.

Risk 2014 – Prioritet 2
Avsaknad av spårbarhet och dokumentation i programförändringsprocessen ökar risken för oönskad funktionalitet eller att otillräckligt testade och felaktiga förändringar utvecklas och införs i produktionsmiljön. Detta i sin tur leder till en ökad risk för fel i de statistiska beräkningarna.

Rekommendation 2014
Vi bedömer att vår iakttagelse från 2012 är delvis åtgärdad. Vi rekommenderar att KPI inför en liknande programförändringsrutin för SAS-skript och Excel-filer som den som används för Pi09. Rutinen bör säkerställa att det finns en tillförlitlig förteckning över genomförda programförändringar samt att det tydligt framgår vem som godkänt förändringen, hur den testats och vem som godkänt att den sattes i produktion. När man gör ändringar i beräkningar rekommenderar vi att KPI behåller en kopia av filen som grundmall. Denna grundmall bör användas som utgångspunkt vid statistikproduktion, och sparas som en kopia när data matats in i filen. På detta sätt kan ändringar i beräkningar och formler skiljas från tillfällen då filen sparats om på grund av inmatning av data. Vidare rekommenderar vi att KPI gör regelbundna uppföljningar genom att ta stickprov på checklistor som gjorts för att följa upp att rutinen följs.

4.3.2 Behörighetsindelningen till filservern är grov

Iakttagelse 2012
Vid vår granskning noterade vi att samtliga anställda inom KPI får behörighet till den nätverksmapp där bland annat indata, Excel-filer och SAS-skript förvaras vid statistikproduktion. Användarna har således inte rollbaserade behörigheter utan kan komma åt all information i mappen.

Status 2014
Vid vår granskning noterade vi att KPI inte genomfört några väsentliga åtgärder avseende denna iakttagelse.

Risk 2014 – Prioritet 2
Att tilldela användare för grova behörigheter innebär en ökad risk för att oavsiktliga fel uppstår genom att en användare öppnar, ändrar eller tar bort en fil som denne inte egentligen behövde för sitt arbete. I en delad nätverksmapp är det också lätt att oavsiktligt flytta filer eller mappar vilket kan leda till att nödvändig information inte går att hitta inom rimlig tid.

Rekommendation 2014
Vi bedömer att vår iakttagelse från 2012 kvarstår, att KPI ser över sina behörighetsroller och undersöker möjligheten att utforma en mer finkornig uppdelning av rollerna baserat på användarens arbetsuppgifter.

4.3.3 Dokumentationen vid programförändringar är inte enhetlig

Iakttagelse 2012
Vid vår granskning noterade vi att vissa typer av programförändringar inte dokumenterades på ett enhetligt sätt. Vissa små förändringar saknade acceptanstest och akuta förändringar hade inte alltid fullständig dokumentation.

Status 2014
Vid vår uppföljning noterade vi att SCB har infört en förvaltningsdagbok där alla förändringar skall loggas, oberoende av vilket typ av förändring ärendet gäller. Detaljer för programförändringar dokumenteras i testverktyget ReqTest där hela processen från beställning till produktionssättning kan följas.

Rekommendation 2014
Vi bedömer vår iakttagelse från 2012 som åtgärdad.

4.3.4 Behörigheter har tilldelats i Pi09 utan underlag

Iakttagelse 2012
Vid vår granskning noterade vi att behörigheter i Pi09 har lagts till under året. Processen går till så att enhetschef meddelar systemadministratörer på enheten vilka behörigheter personer ska tilldelas via e-post. Däremot noterade vi att dessa e-postmeddelanden inte sparas på ett enhetligt sätt. Detta innebär att det inte är möjligt att i efterhand se att användare innehar de behörigheter som de ska ha blivit tilldelade.

Status 2014
Vid vår uppföljning noterade vi att det finns en ny rutinbeskrivning för behörighethantering i Pi09. Vid vår granskning observerade vi att samtliga behörighetsbeställningar sparas på en central plats.

Rekommendation 2014
Vi bedömer vår iakttagelse från 2012 som åtgärdad.

4.4 Arbetskraftsundersökningarna

4.4.1 Spårbarheten vid programförändringar i AKU-systemen, SAS-skript och Excel-filer är otillräcklig

Iakttagelse 2012
Vid vår granskning noterade vi att det inte var möjligt att få ut en tillförlitlig förteckning över de programförändringar som genomförts i AKU-systemen, i SAS-skript och i Excel-filer under året. Vidare noterade vi att beställningar, tester och godkännanden av programförändringar inte regelmässigt dokumenteras och sparas. I den dokumentation som finns framgår inte vem som beställt en förändring. Vi noterade även att tester i vissa fall dokumenterades i ReqTest men att det inte är tydligt när detta verktyg ska användas.

Status 2014
Vid vår uppföljning noterade vi att ingen förändring beträffande Excel-filerna har skett sedan 2012, de används endast för utdata. SCB har dock börjat använda Sharepoint som en gemensam yta för ärendehantering. Där ska ändringsbegäran för SAS-skripten som ska innehålla ändringen och lösningsförslag läggas upp. Vid vår granskning noterade vi att ett av nio stickprov saknade dokumenterad testning i ändringsbegäran. Vidare framgick det inte alltid i ändringsbegäran vem som utfört testningen.

Risk 2014 – Prioritet 3
Avsaknad av spårbarhet och dokumentation i programförändringsprocessen ökar risken för oönskad funktionalitet eller att otillräckligt testade och felaktiga förändringar utvecklas och införs i produktionsmiljön. Detta i sin tur leder till en ökad risk för fel i de statistiska beräkningarna.

Rekommendation 2014
Vi bedömer att vår iakttagelse från 2012 är delvis åtgärdad. Vi noterade dock att visst förbättringsutrymme kring efterlevnad av rutinen kvarstår. Vi rekommenderar att AKU fortsätter att följa sin programförändringsrutin som säkerställer samt säkerställer att det finns en tydlig samt tillförlitlig förteckning över vilka som genomfört förändringen från beställning till produktion. Vidare rekommenderar vi att rutinen införs för alla typer av förändringar, oavsett om ändringen rör AKU-systemen, SAS-skript eller Excel-filer.

4.4.2 Spårbarheten vid behörighetsbeställning är otillräcklig

Iakttagelse 2012
Vid vår granskning noterade vi att det inte alltid gick att hitta beställningar av behörigheter för användare som lagts till under året.

Status 2014
Vid vår uppföljning noterade vi att behörigheter beställs genom Beställarportalen bortsett från databasbehörigheterna som fortfarande beställs via epost.

Rekommendation 2014
Vi bedömer vår iakttagelse från 2012 som åtgärdad.

4.4.3 Excel-filer som används vid statistikproduktion är inte låsta

Iakttagelse 2012
AKU använder en viss struktur i sina Excel-filer som anger var användaren ska fylla i information och vilka celler som inte ska ändras. Detta anges genom en visuell markering som hjälper till att förhindra oavsiktliga förändringar eller fel på grund av okunskap. Denna markering är dock inte tillräcklig för att förhindra oavsiktliga fel och ändringar som kan uppstå i samband med det löpande arbetet.

Status 2014
Vid vår uppföljning noterade vi att AKU infört skrivskydd i Excel-mallarna. För ett av våra stickprov saknades skrivskydd på cellnivå, denna iakttagelse har dock åtgärdats av SCB under granskningen 2014. Vidare noterade vi att förändringar i Excel-mallarna enligt rutin ska loggas i en Wordfil som finns tillgänglig i Sharepoint.

Rekommendation 2014
Vi bedömer vår iakttagelse från 2012 som åtgärdad med hänsyn till de åtgärder som genomförts under granskningen.

4.5 Betalningsbalansen

4.5.1 Spårbarheten vid programförändringar i Buster[1], SAS-skript och Excel-filer är otillräcklig

Iakttagelse 2012
Vid vår granskning noterade vi att det inte var möjligt att få ut en tillförlitlig förteckning över programförändringar som genomförts i SAS-skript och Excel-filer under året. Vidare noterade vi att beställningar, tester och godkännanden av programförändringar inte regelmässigt dokumenteras och sparas. Vi noterade även att dokumentationen av godkännande för produktionssättning inte alltid dokumenterades i ärendehanteringssystemet vid förändringar i Buster.

Status 2014
Datahanteringssystemet, Buster, har varit under avveckling sedan 2012. Vid vår uppföljning hade det nya systemet, FMBoP, satts i drift. Dock drivs det ännu i projektform och har ej kommit in i förvaltning. Därav saknas underlag för att bedöma om iakttagelsen har åtgärdats.

Risk – Prioritet 1
Avsaknad av spårbarhet och dokumentation i programförändringsprocessen ökar risken för oönskad funktionalitet eller att otillräckligt testade och felaktiga förändringar utvecklas och införs i produktionsmiljön. Detta i sin tur leder till en ökad risk för fel i de statistiska beräkningarna.

Rekommendation 2014
Vi bedömer att vår iakttagelse från 2012 kvarstår. Vi rekommenderar att BoP inför en formaliserad programförändringsrutin för SAS-skript och Excel-filer som säkerställer att det finns en tillförlitlig förteckning över genomförda programförändringar samt att det tydligt framgår vem som godkänt förändringen, hur den testats och vem som godkände att den sattes i produktion. Vidare rekommenderar vi att BoP säkerställer att programförändringar av FMBoP, när det övergår i förvaltning, tydligt dokumenteras så att det tydligt framgår vem som godkänt testning och produktionssättning av en förändring.

4.5.2 Regelbundna genomgångar av behörigheter i Buster dokumenteras ej

Iakttagelse 2012
BoP genomför regelbundna genomgångar av behörigheter till Buster genom systemgenererade listor av behörigheter i den underliggande databasen. Vid vår granskning noterade vi att denna genomgång inte dokumenteras.

Status 2014
Vid vår granskning noterade vi att SCB centralt har definierat ägare för samtliga databaser. Vid den centrala behörighetsgenomgången skickas listan ut på ägarbasis. Listorna skickas ut från säkerhetsorganisationen till respektive enhetschef som uppdaterar listan utefter aktuella behörigheter och sedan skickas listan tillbaka till säkerhetsorganisationen med information om behörigheter som bör korrigeras, se iakttagelse 4.1.3.

Rekommendation 2014
Vi bedömer vår iakttagelse från 2012 som åtgärdad.

[1] Vid uppföljningen 2014 har vi genomgående granskat systemet FMBoP istället för Buster

4.5.3 Bristande spårbarhet vid behörighetsbeställningar till Buster

Iakttagelse 2012
BoP har en rutin för att dokumentera beställningar och godkännande av nya behörigheter till Buster. Vid vår granskning noterade vi ett antal gällande behörigheter som inte hade dokumenterade beställningar eller godkännanden.

Status 2014
Vid vår uppföljning noterade vi att samtliga behörigheter inom BoP enligt rutin ska beställas genom Beställarportalen. I vår granskning noterade vi dock att det saknades beställningar för vissa nya användare.

Risk 2014 – Prioritet 2
Avsaknaden av komplett och korrekt dokumentation över vilka behörigheter som godkänts och som bör vara giltiga i systemet ökar risken för att obehöriga användare inte upptäcks i tid. Detta i kombination med att de regelbundna genomgångarna inte dokumenteras ökar risken för att felaktiga behörigheter inte upptäcks och åtgärdas.

Rekommendation 2014
Vi bedömer att vår iakttagelse från 2012 är delvis åtgärdad. Vi rekommenderar att BoP följer upp tillämpningen av behörighetsbeställningsrutinen för att säkerställa att alla behörigheter i systemet är beställda och godkända enligt gällande rutin.

4.5.4 Behörigheter till Busters programfiler omfattas inte av behörighetskontroller

Iakttagelse 2012
Vid vår granskning noterade vi att Busters programfiler förvaras på en nätverksmapp som inte omfattas av de kontroller som täcker behörigheter till BoP:s övriga grupper i Active Directory. Vid granskningen noterade vi obehöriga grupper med användare som hade skrivrättigheter till Busters programfiler.

Status 2014
SCB är i takt med att ersätta det tidigare beräkningssystemet Buster med det nya beräkningssystemet, FMBoP. Behörigheter för programfiler hanteras dock på samma sätt för Buster och FMBoP. I vår granskning noterade vi att obehöriga grupper hade skrivrättigheter till FMBoPs programfiler.

Risk 2014 – Prioritet 2
Genom att användare som inte behöver åtkomst till Busters programfiler har behörighet till nätverksmappen ökar risken för att filer oavsiktligt flyttas, ändras eller tas bort vilket kan leda till att Buster blir otillgängligt för användarna.

Rekommendation 2014
Vi bedömer att vår iakttagelse från 2012 kvarstår. Vi rekommenderar att BoP ser över och rensar bort inaktuella och felaktiga behörigheter på den aktuella nätverksmappen. Vidare rekommenderar vi att BoP inför samma behörighetskontroller som gäller för andra nätverksmappar även på den yta där Busters och FMBoPs programfiler förvaras.

Bilaga A Respondenter och dokumentgranskning

Respondenter

Befattning	Statistikprodukt
Identitet och behörighetsansvarig SCB	Generell
Vikarierande biträdande generaldirektör SCB	Generell
Avdelningschef IT-avdelningen	Generell
Databasadministratör	Generell
IT-drift	Generell
IT-säkerhetsansvarig	Generell
Avdelningschef för Befolkning och välfärd	AKU
Produktionssystemsansvarig	AKU
Produktansvarig och biträdande enhetschef	AKU
IT-koordinator	AKU
Metodansvarig	AKU
Produktansvarig BoP	BoP
Projektledare för FMBoP	BoP
IT-koordinator mot avdelningen ekonomisk statistik	BoP
IT och systemansvarig KPI	KPI
Enhetschef	KPI
IT superuser Pi09	KPI
Kvalitetsansvarig för NR	NR
Förvaltningsansvarig för NR	NR
Enhetschef för NR	NR
IT-koordinator NR	NR

Granskade dokument

Namn	Datum
Riktlinjer för styrning av kommunikation och drift	2014-10-08
Instruktion för datahallar	2014-10-08
Behörighetsrutin för databaser	2014-10-27
Rutin för ändring av administratörslösenord	2014-12-03